a digital signal processor (DSP); an application specific integrated circuit (ASIC); a field programmable gate array; and a microcontroller.

[0108] FIG. **5** shows a flow chart illustrating a method in a cellular terminal, according to an example embodiment, comprising:

[0109] transmitting **510** a request that requires authentication procedure triggering to a cellular network and responsively receiving **520** from the cellular network an authentication request message with an indication of a selected cryptographic algorithm from a group of a plurality of cryptographic algorithms;

[0110] attempting to decode **530** the authentication request message to a decoded authentication request according to the selected cryptographic algorithm and based on a shared secret known by the cellular terminal and a network operator of the cellular terminal;

[0111] producing a determination **540** whether the attempt was successful and the cellular terminal supports the selected cryptographic algorithm in authenticating to the cellular network; and

[0112] in case the determination is positive, based on the decoded authentication request, the shared secret and the selected cryptographic algorithm, producing and encrypting an authentication response message and transmitting the authentication response message to the cellular network, **550**; and

[0113] in case the determination is not positive, producing and sending to the cellular network a failure report, **560**.

[0114] The failure report can be formed in a number of ways and in a variety of different forms. For example, in an example embodiment, the failure report comprises and/or consists of authentication failure message. In an example embodiment, the authentication failure message comprises any of: a protocol discriminator; a security header type; an authentication failure message type; an EPS mobility management, EMM, cause; and an authentication failure parameter.

[0115] In an example embodiment, the cellular terminal is configured to detect an error in a message authenticator of the authentication requests, MAC-A. In an example embodiment, the cellular terminal is configured to produce the failure report in a manner dependent on the error that was likely to prevent successful decoding of the authentication request or the use of the selected cryptographic algorithm.

[0116] In an example embodiment, the cellular terminal is configured to contain in the failure report, if the error was caused by incompatible length of MAC-A: an indication of the length of at least one of: the TUAK MAC-A used by the cellular terminal; and the TUAK MAC-A that the cellular terminal derives as likely used by the cellular network in the authentication request.

[0117] In an example embodiment, the failure report comprises a new information element for error reporting. In an example embodiment, the error reporting indicates a new EMM cause code. In an example embodiment, the error reporting indicates an existing EMM code such as #20.

[0118] In an example embodiment, the cellular terminal is configured to detect an error in an authentication management field. In an example embodiment, the authentication management field is contained by the MAC-A.

[0119] In an example embodiment, the failure report indicates any one or more of: the length of TUAK MAC-A used by the cellular terminal; the length of TUAK MAC-A the cellular terminal presumes network used; the length of TUAK integrity key used by the cellular terminal; the length of TUAK integrity key the cellular terminal presumes network used; the length of TUAK cipher key used by the cellular terminal; the length of TUAK cipher key the cellular terminal presumes network used; the length of TUAK authentication value (e.g. RES) used by the cellular terminal; the length of TUAK authentication value (e.g. RES); the cellular terminal presumes network used; the length of TUAK shared secret key used by the cellular terminal; and the length of TUAK shared secret key the cellular terminal presumes network used.

[0120] In an example embodiment, the cellular terminal is configured to detect an error in a re-synchronization token.

[0121] In an example embodiment, the failure report contains an indication of the re-synchronization token as computed by the cellular terminal.

[0122] In an example embodiment, the cellular terminal is configured to detect that the authentication request is configured to request the cellular terminal to use an authentication algorithm that is not supported by the cellular terminal.

[0123] In an example embodiment, the failure report comprises any one or more of: an indication authentication algorithm or algorithms supported by the cellular terminal; and an indication of authentication algorithm or algorithms requested by the network as determined by the cellular terminal.

[0124] Without in any way limiting the scope, interpretation, or application of the claims appearing below, a technical effect of one or more of the example embodiments disclosed herein is that reasons for authentication failures may be identified to the cellular network for suitable action therein. Another technical effect of one or more of the example embodiments disclosed herein is that cellular networks may test different authentication algorithms and/or parameters and learn from failure reports the capabilities of cellular terminals. Another technical effect of one or more of the example embodiments disclosed herein is problems caused for cellular terminals by using two or more different authentication procedures may be identified and addressed by the cellular network.

[0125] Embodiments of the present invention may be implemented in software, hardware, application logic or a combination of software, hardware and application logic. In the context of this document, a "computer-readable medium" may be any non-transitory media or means that can contain, store, communicate, propagate or transport the instructions for use by or in connection with an instruction execution system, apparatus, or device, such as a computer, with one example of a computer described and depicted in FIG. **3** or **4**. A computer-readable medium may comprise a computer-readable storage medium that may be any media or means that can contain or store the instructions for use by or in connection with an instruction execution system, apparatus, or device, such as a computer.

[0126] If desired, the different functions discussed herein may be performed in a different order and/or concurrently with each other. Furthermore, if desired, one or more of the before-described functions may be optional or may be combined.

[0127] Although various aspects of the invention are set out in the independent claims, other aspects of the invention comprise other combinations of features from the described